REDUNDANCY-BASED ELECTRONIC DEVICE HAVING CERTIFIED AND NON-CERTIFIED CHANNELS

Background Information

The present invention relates to an electronic device having at least two channels, preferably a dual-channel programmable logic circuit, with it being possible for this programmable logic circuit to be, for example, the central processing unit of a stored-program control.

Electronic devices for safety-related tasks require a high level of functional safety, with the term "functionally safe" being based on the term "functional safety" used in the international publication Draft-IEC 1508.

A key feature of functionally safe electronic devices is that they include special means for avoiding, detecting and handling errors and malfunctions.

A common way to avoid, detect and handle errors and malfunctions is to design multi-channel redundancy-based electronic devices, in which the same operations are carried out in parallel in all the channels. Results and output values are compared to determine whether an error has occurred in one of the channels.

One particular group of errors that is particularly significant if one is striving to guarantee functionally safe operation is systematic errors in modules, units or components of channels. Errors of this kind may be caused, for example, by the logic structure, i.e. the way the individual

components and modules are interconnected, or by their physical characteristics, which are governed by the manufacturing process used. Extensive certification is required to prove that the application in question is sufficiently free of systematic errors.

Semiconductor technology changes very rapidly nowadays, and manufacturing processes are modified after very short periods of time. As a result, one often has to take repeated action to prove that the components and units in question are free of systematic errors because components and units of this kind must be subjected to extensive certification before they can be used in systems to be rated functionally safe.

Because of the rapid innovation cycle in the semiconductor industry, this certification has to be carried out afresh for each new generation of microprocessor or memory chip, for example, with the certification process taking considerable time, as tests must be performed and/or it has to be proven that the component in question functions properly resulting in a considerable delay before new types of components can be used in safety-related applications.

The object of the present invention is therefore to produce an electronic device that allows the use of modules, units or components not yet proven sufficiently free of systematic errors in safety-related systems having homogeneously redundant channels.

This object is achieved for the electronic device in that the at least dual-channel homogeneous-redundancy-based electronic

device, which preferably may be a dual-channel homogeneous-redundancy-based programmable logic circuit, has at least one certified channel and at least one non-certified channel, and the certified channel is a channel that is sufficiently free of systematic errors.

Here a "channel sufficiently free of systematic errors" is understood to mean a channel for which, over a specific period of time, the probability of failure does not exceed a specific level as determined by the application in question, e.g. a level as defined in the international publication Draft-IEC 1508.

If a queriable signal, e.g. a special memory cell or a mechanical or electronic switch, is provided for each channel, and when the signal is queried a first flag denoting a certified channel or a second flag denoting a non-certified channel is detectable, and the electronic device only starts to operate if the first flag is detected at least once when the flags of the individual channels are queried, this constitutes a self-test of the electronic device that ensures that the electronic device only starts to operate if it is guaranteed that at least one of the channels of the at least dual-channel electronic device is a channel sufficiently free of systematic errors, i.e. a certified channel.

If the querying of flags of the individual channels is carried out in sequence, it can be determined unambiguously which of the channels is a channel sufficiently free of systematic errors, i.e. a certified channel, and which of the channels is

a channel insufficiently free of systematic errors, i.e. a non-certified channel.

When the electronic device is in operation, if, after a preassignable period of time during which no errors were detected, the flag of the non-certified channel can be switched over from the second flag denoting that the channel is non-certified to the first flag denoting that the channel is certified, this channel can itself be used as the reference channel after a sufficiently long period of operation and evaluation of the operating behavior of the hitherto non-certified channel, so that the electronic device allows use of, for example, units, components or modules of the next generation but one which have of course not been certified, without any need to prove in advance that they are free of errors.

Further advantages and inventive elements are explained below in the description of an exemplary embodiment, with the help of the drawing and in conjunction with the dependent claims.

In particular, Figure 1 shows a block diagram of a dual-channel homogeneous-redundancy-based central processing unit of a stored-program control.

According to Figure 1, the electronic device EG is a dual-channel homogeneous-redundancy-based central processing unit of a stored-program control. Here, "homogeneous redundancy" means that the individual channels are symmetrical and have at least functionally equivalent units, components or modules.

In the exemplary embodiment shown in Figure 1, channel A has a microprocessor P, a program memory I and a data memory R. A monitoring unit W, a watchdog, monitors operation of microprocessor P. Channel B is homogeneously redundant with respect to channel A which is particularly clear from the fact that the same components P, I and R are given the same reference letters.

Channel A must include components P, I, R and W that have been proven sufficiently free of systematic errors, meaning that the components, units and modules are certified. Thus channel A as a whole constitutes channel A that is sufficiently free of systematic errors.

In channel B, one or a plurality of components P, I, R, and W which have been modified in some way, i.e. due to a new or modified manufacturing process, and which have not yet been proven sufficiently free of systematic errors, are used.

If any systematic errors present in the relevant units, components or modules of channel B occur, they are detected when results are compared with those of channel A, which can be carried out by coupling K located between channels A and B, and can thus be handled appropriately.

It is thus possible to use units, components or modules not yet proven sufficiently free of errors and therefore not yet certified in a channel A, B in redundancy-based electronic device EG without impairing its safety characteristics.

Systematic errors caused by, for example, the physical characteristics of the electronic units, components or modules in question or by modifications to the manufacturing or assembly process can be detected via comparison of results.

Electronic device EG according to the present invention allows the manufacturer of such a device to react immediately to innovation cycles, for example in the semiconductor industry, and also, in functionally safe systems, to always offer units, components or modules that correspond to the current state of development, even if these units have not yet been certified and thus explicitly proven sufficiently free of systematic errors.

It is also especially advantageous in this context that this certification can be achieved implicitly via the method according to the invention and electronic device EG according to the invention.

To this end, a flag denoting whether channel A, B in question can be considered sufficiently free of systematic errors is provided for each channel A, B of electronic device EG. After a specific period of time preferably freely assignable by the user during which no systematic errors have been detected in the hitherto non-certified channel A, B during operation of electronic device EG, this flag can be switched over from 'non-certified' to 'certified,' so that the hitherto not explicitly certified channel, which has been shown to be sufficiently free of systematic errors during actual operation, can also be used like an explicitly certified channel.

This allows one, preferably in an electronic device EG, to also use, along with what is now an "online-certified" channel, units, modules or components of the next semiconductor component generation but one in a further redundant channel A, B and where possible to use the method described above to prove that these components too are sufficiently free of systematic errors.

Thus electronic device EG according to the invention and the process according to the invention allows use of cutting-edge units, modules or components which would otherwise only be authorized after a lengthy certification process concerning use in safety-related systems.